

Recipe 10 - Importing Browser and Server Certificates

Table of Contents

1	Introduction	1
1.1	View Installed Certificates through Internet Explorer	2
2	Importing User Certificates into a Browser.....	4
2.1	Importing a PKCS #12 User Certificate.....	9
3	Configure IIS server for SSL with Client Authentication	16
3.1	Create a Server Certificate Request	16
3.2	Import Server Certificate into IIS	26

Version 2.0.0

1 Introduction

A certificate is a digital statement issued by an authority that vouches for the identity of the holder of a private key. A certificate binds a public key to the identity of the person, computer, or service that holds the corresponding private key. Certificates often contain other information related to the public key, such as identity information about the entity that has access to a corresponding private key. Certificates are widely distributed, can be issued by numerous parties, and examined for verification without referring to a centralized database. The issuer of a certificate is attesting to the validity of the relationship using its public key and a private issued certificate.

As discussed in the Technical Approach for the Authentication Service Component document, certificates are needed to properly configure all Agency Applications (AAs). The specific uses for the certificates will differ, however, depending upon the assurance level of the application (high assurance/low assurance).

For assurance levels 1 & 2, E-Governance Certificate Authority (E-GCA) server certificates are required to provide a secure, trusted link between the AA and the Credential Service Provider (CSP). Certificates serve two purposes – to encrypt (and secure) the identity assertion during transmission, as well as to assert the identities of the servers themselves.

FBCA certificates are required for assurance levels 3 & 4 for Public Key Infrastructure (PKI) identity management of both the end user and the AA's web server. End users will present credentials via digital certificates, which will be verified via path discovery and validation to confirm authenticity and validity. In exchange, the AA's web server provides a certificate to reassure the end user that the server is indeed the legitimate server.

For more information regarding certificates and their role in E-Authentication, please visit the E-Authentication website at www.cio.gov/eauthentication.

This configuration guide assumes the following:

- a. You are familiar with the role of certificates in the architecture
- b. You are likely a systems engineer or consultant with integration experience and a strong understanding of the technical settings which will be changed.
- c. You have access (either directly or through another party) to make necessary configuration changes to any required network configurations, if needed.

1.1 View Installed Certificates through Internet Explorer

One of the first steps in this recipe is to review the certificate “store” on the local computer. This is an important step, as it familiarizes you (the user) with the process of accessing, viewing, and updating the certificates on your workstation.

Note: This process is designed for users with Internet Explorer running on a Microsoft Windows platform.

To see imported certificates, open Internet Explorer

- Click on *Tools*
- Then click on *Internet Options*
- Next click on the *Content* tab (see figure 10-1)
- Click on *Certificates* button to view imported certificates (see figure 10-2)

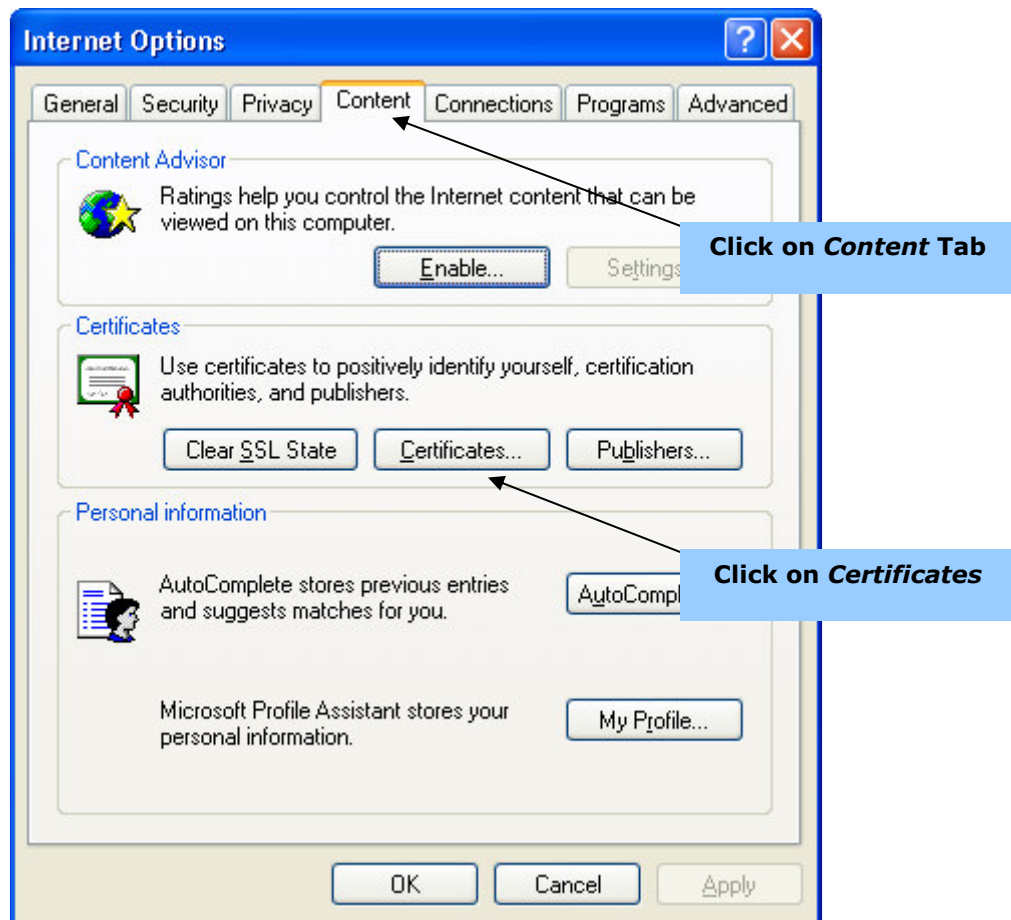


Figure 10-1: Using Internet Options to check certificates

After you click on the *Certificates* button, a window similar to Figure 10-2 will display, revealing the various certificates. Installed certificates belonging to the current user are visible under the *Personal* tab. You can add more certificates to the Personal category if you are logged in as the Administrator. *Other People* refers to the other users on the computer. See Windows information on associating certificates with specific users.

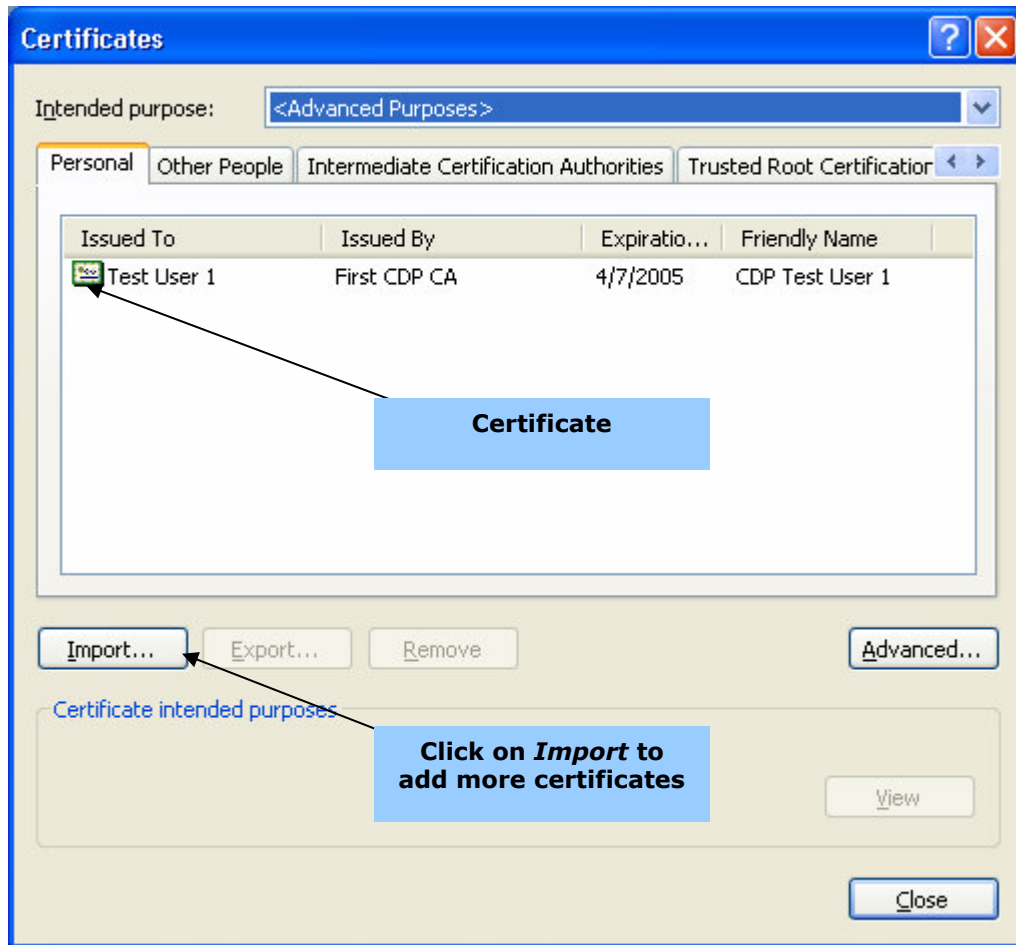


Figure 10-2: List of Certificates

2 Importing User Certificates into a Browser

Now that you're familiar with where certificates are stored on your local machine and how to gain access to them, the next step is to actually import your certificate for use with your web browser.

If it's not already open, double click on the Certificate file that you want to import into your browser.

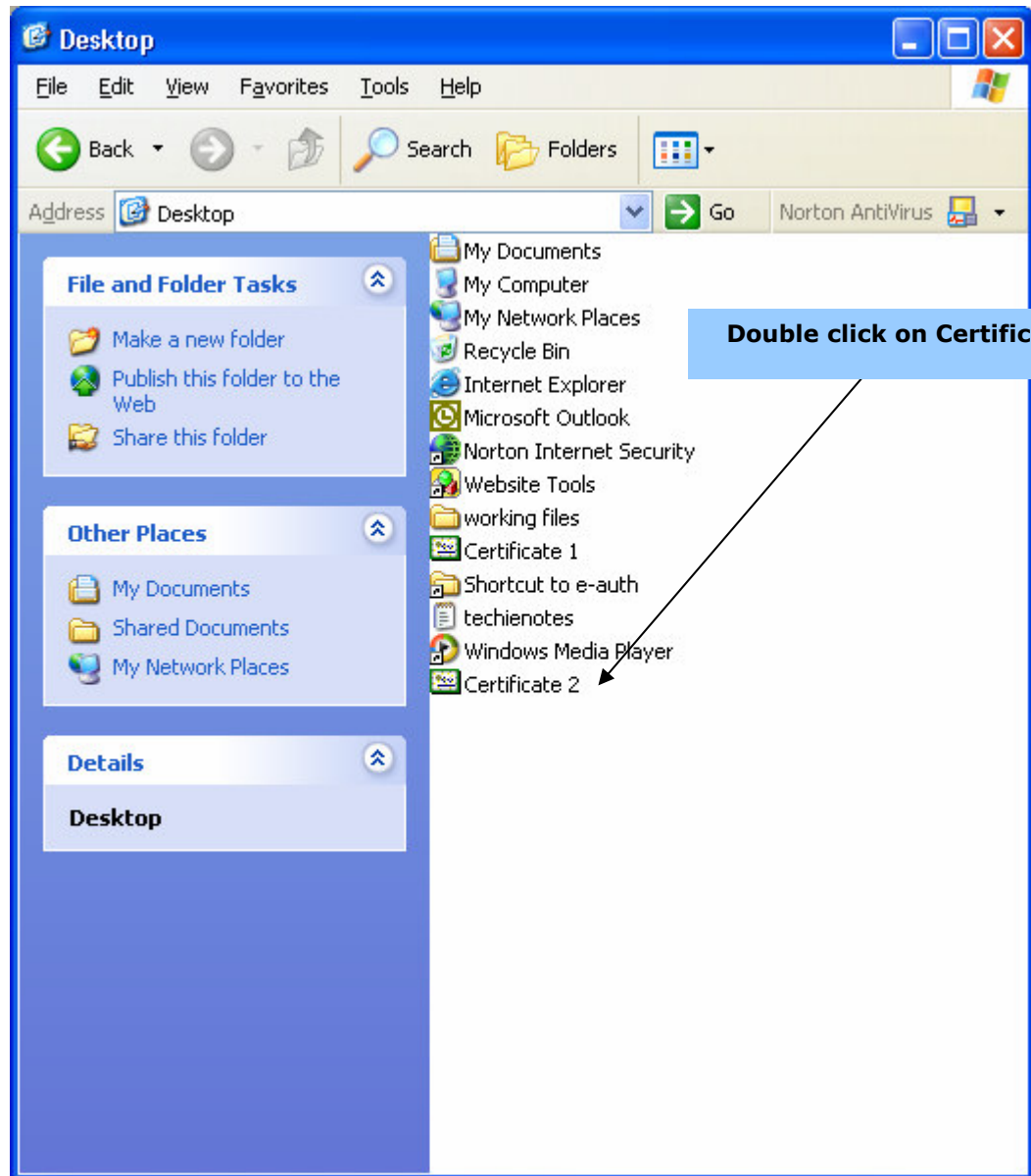


Figure 10-3: Import Certificate

The certificate properties will display, as shown in figure 10-4. After the Certificate properties window displays, click on the *Install Certificate* button.

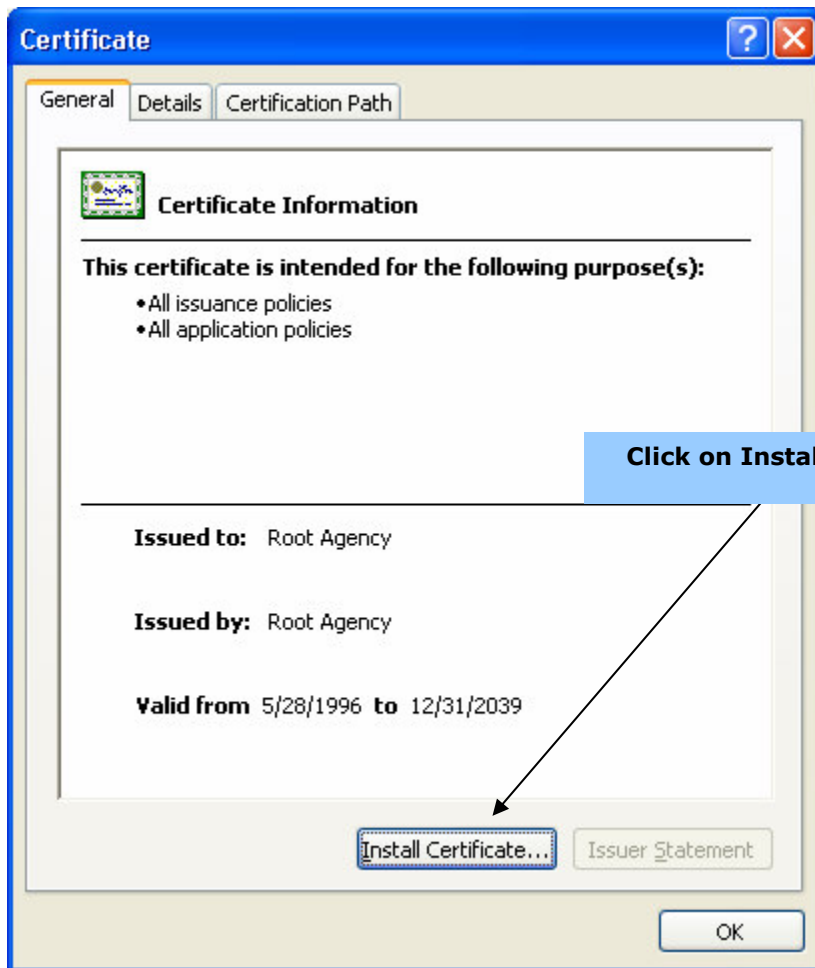


Figure 10-4: Certificate Information

After you click on the *Install Certificate* button, the Certificate Import Wizard will start up, as shown in figure 10-5. This wizard will walk you through the process of importing your certificate.

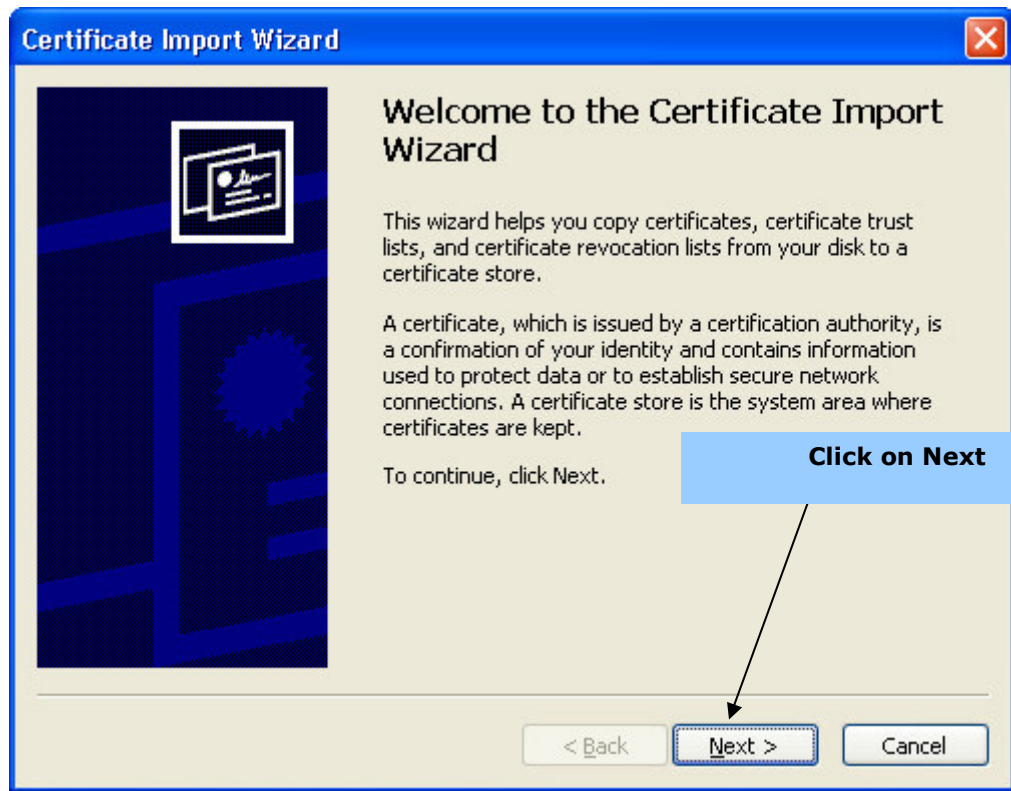


Figure 10-5: Certificate Import Wizard

After the wizard starts, click on *Next*.

When the certificate store options display, allow Windows to automatically select a certificate store. Select *Automatically select the certificate store based on the type of certificate*, and click on *Next*.

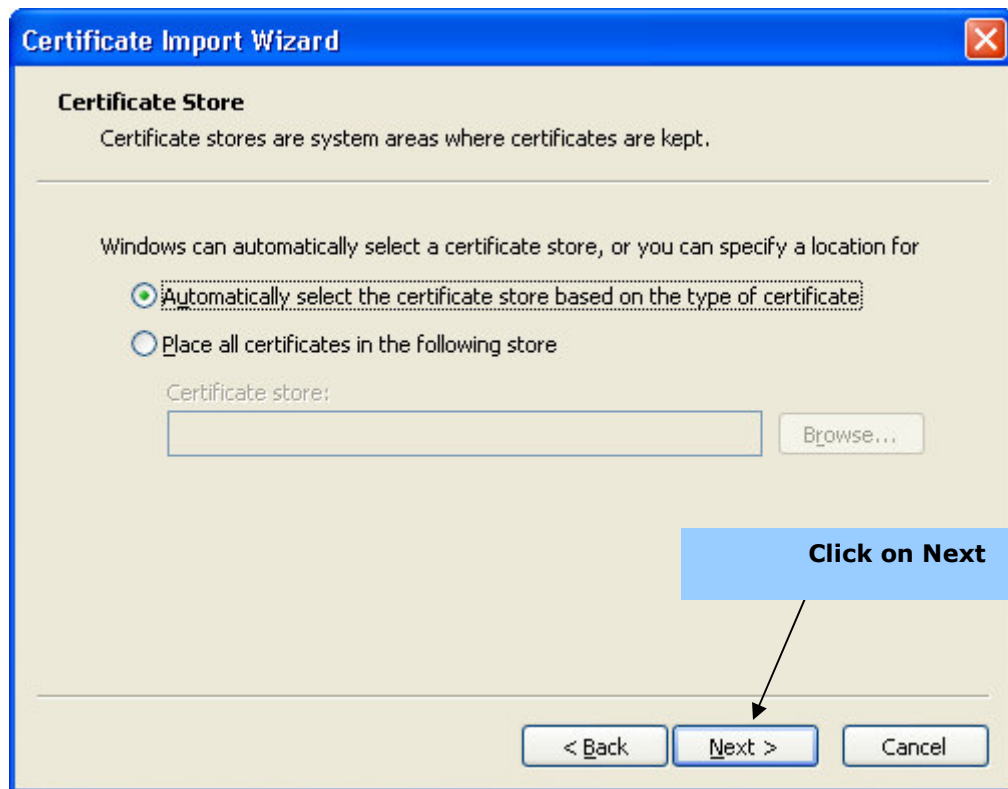


Figure 10-6: Certificate Store

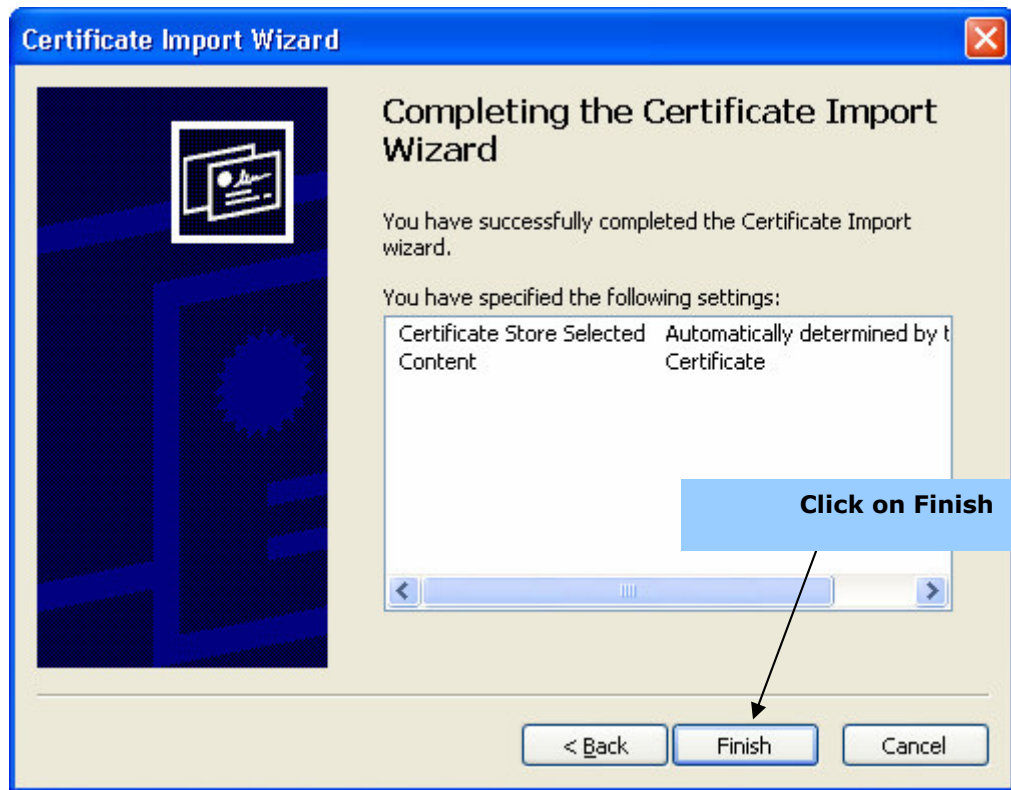


Figure 10-7: Complete the Certificate Import Wizard

Click on *Finish* to complete the import wizard. If the import was successful, a window will display, as shown in figure 10-8.



Figure 10-8: Successful Import

After you click on *OK*, you will be finished importing the user certificate into your browser.

2.1 Importing a PKCS #12 User Certificate

PKCS #12 certificates are a type of certificate that combines both private and public key certificates. The PKCS 12 file is protected by a password, which is made by the creator of the file. To import a PKCS12 Certificate into your browser, start by double clicking on the PKCS12 Certificate you want to import, the Import wizard will begin running.

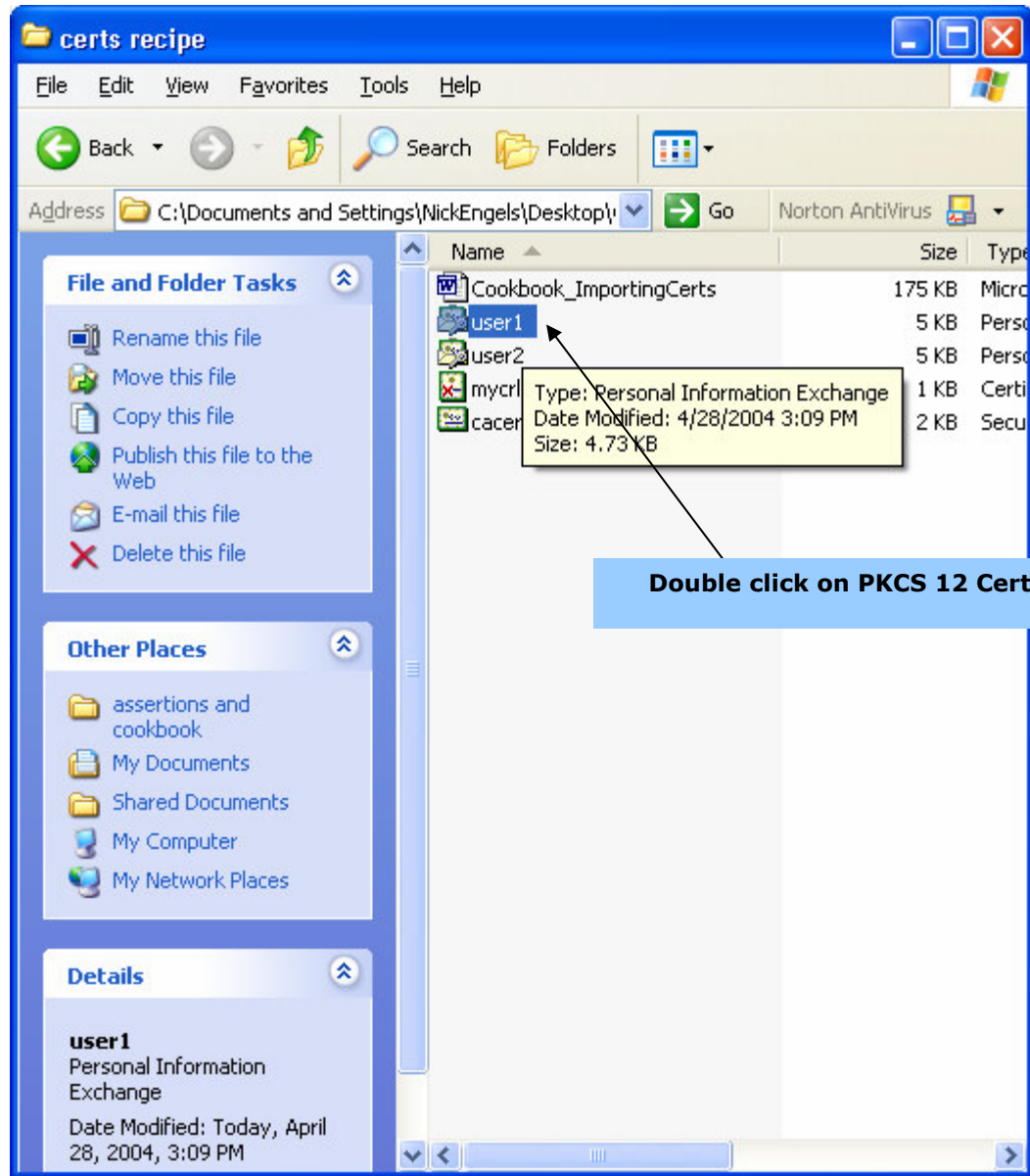


Figure 10-9: Select PKCS12 Certificate

Click *Next* to begin working with the Certificate Import Wizard.

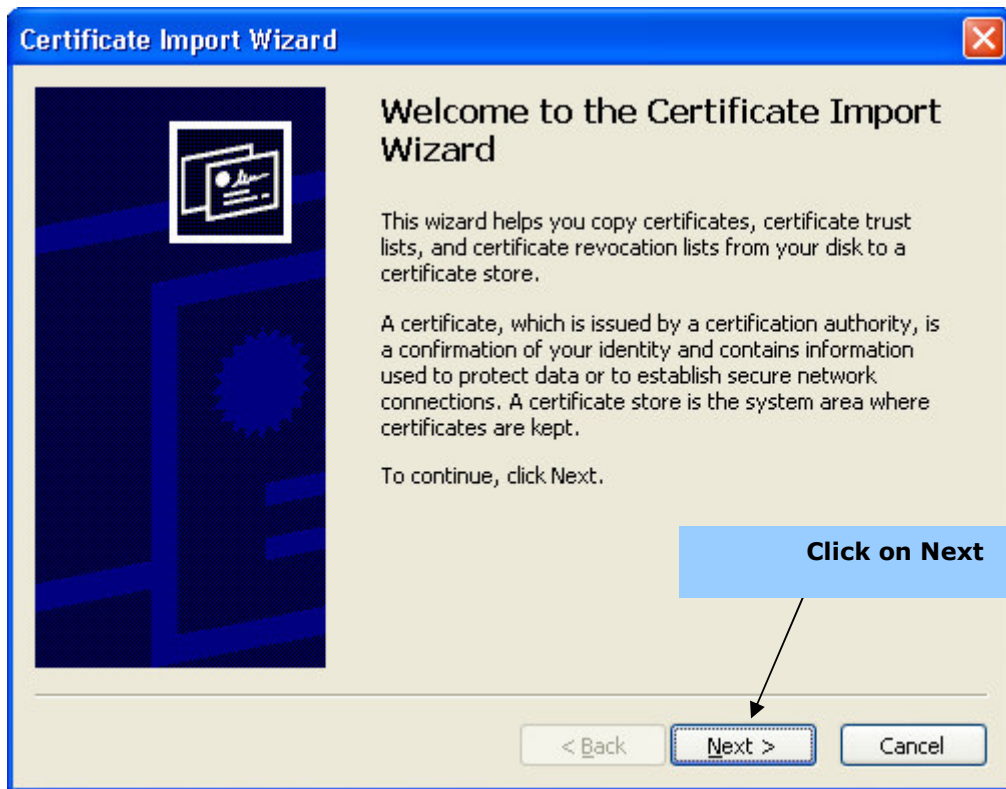


Figure 10-10: Cert Import Wizard

The file you double clicked should already be in the file name box, but if not, click on the *Browse* button and select the certificate file you want to import. After you have selected your PKCS #12 file, click on the *Next* button.

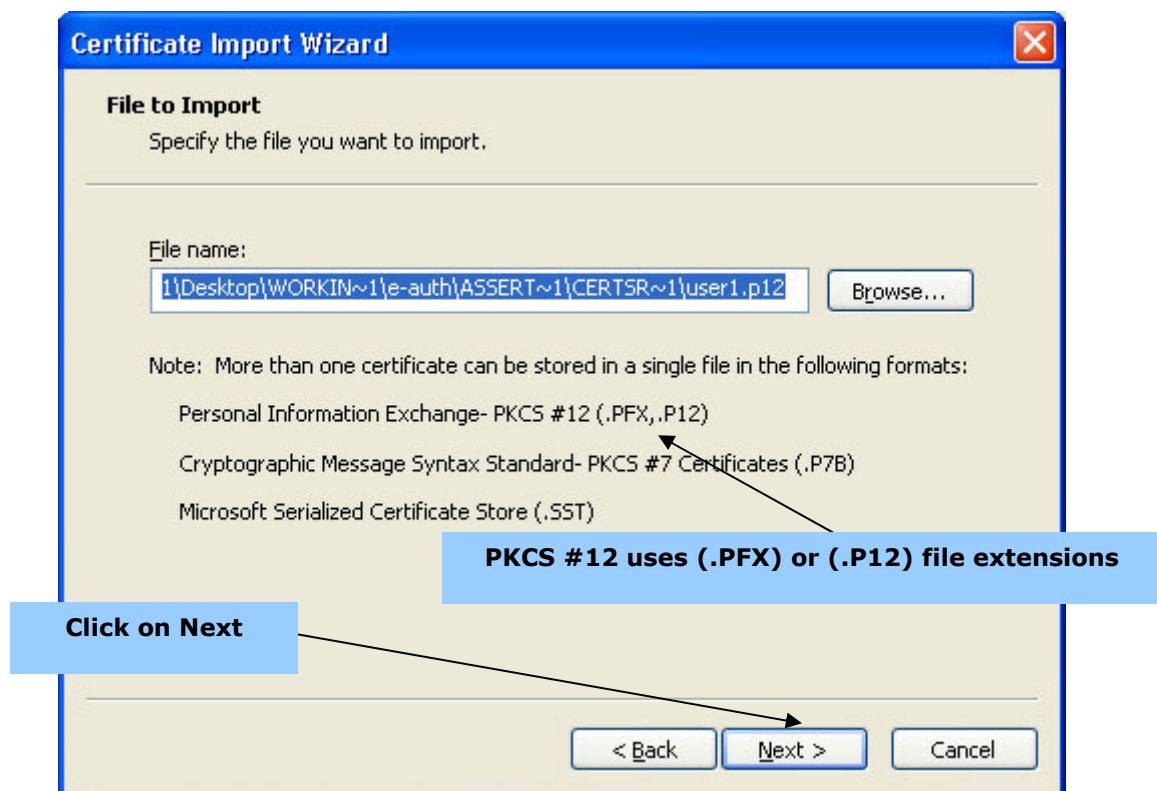


Figure 10-11: Select file to import

To import a PKCS #12 certificate, you must have the password. The password is created when the certificate is made. Enter the password and click on the *Next* button.

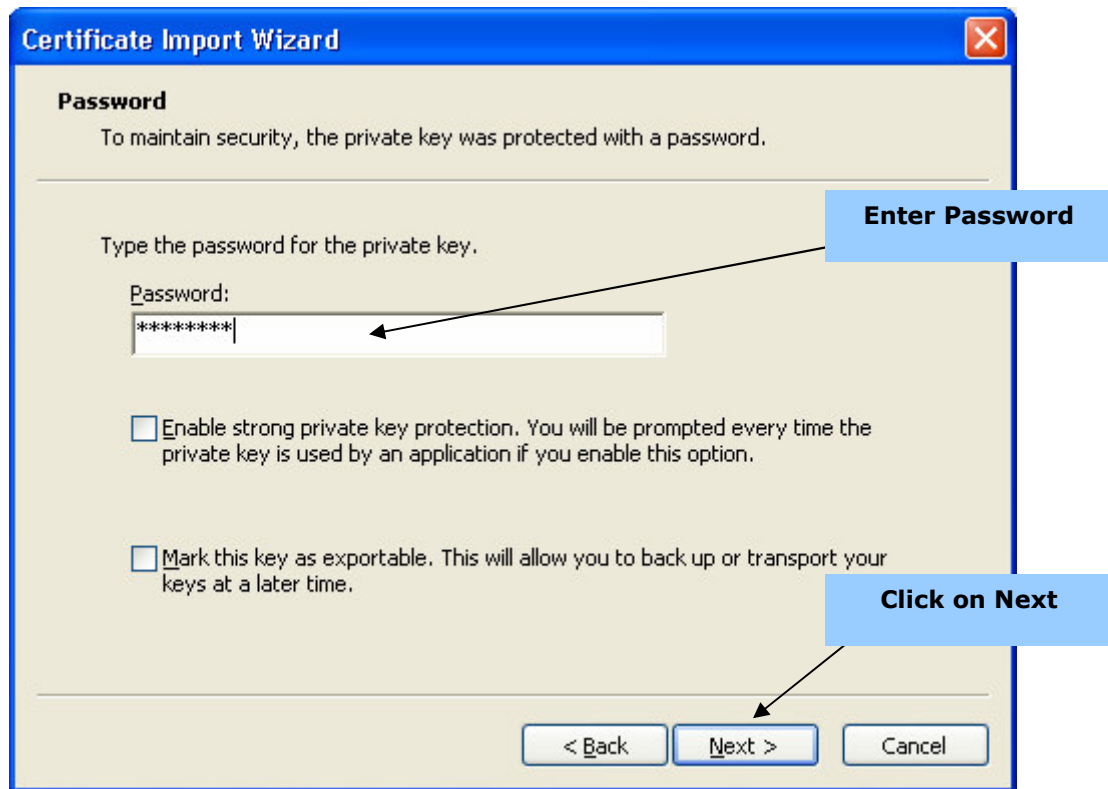


Figure 10-12: Enter Password

After you enter the password, choose to automatically select the certificate store based on the type of certificate. After selecting automatic, as shown in figure 10-13, click on the *Next* button.

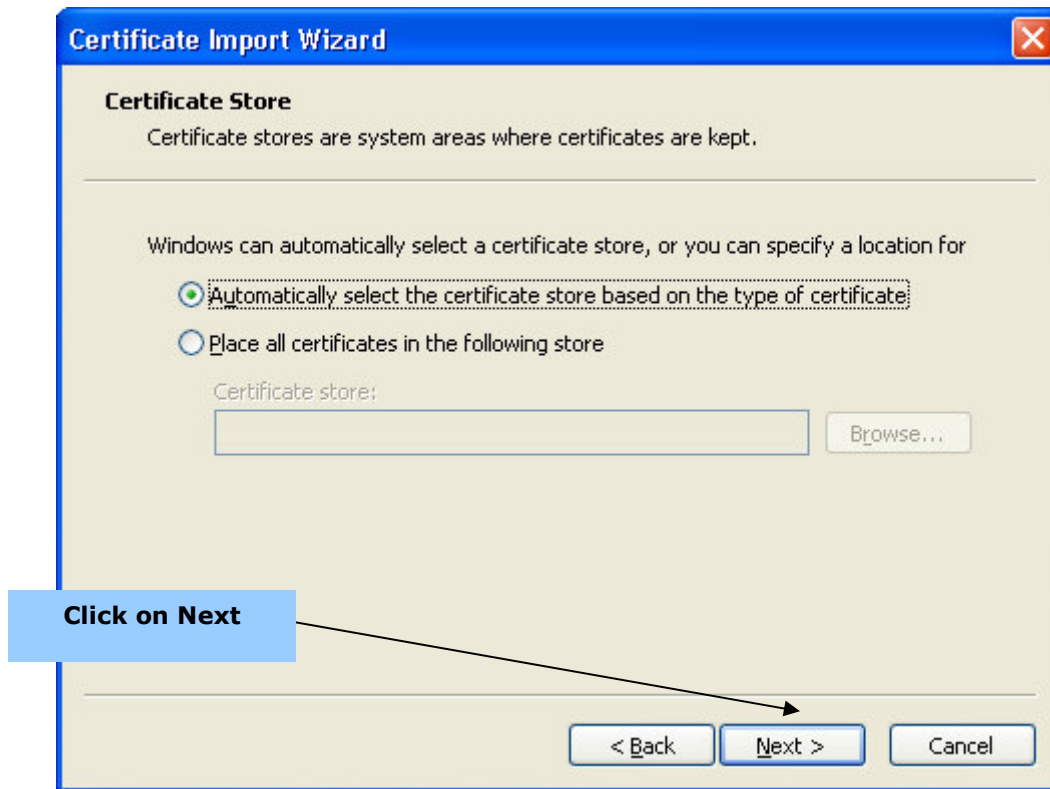


Figure 10-13: Certificate Store

After selecting store settings, click on the *Finish* button, as shown in figure 10-14.

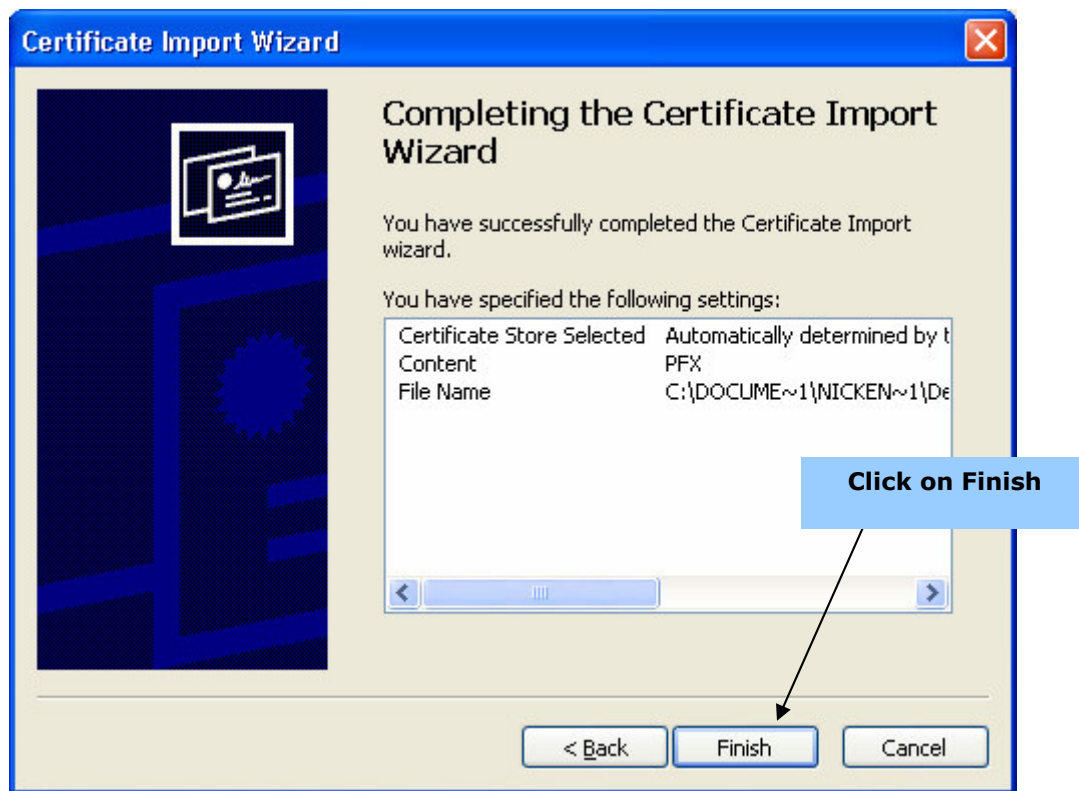


Figure 10-14: Complete the Import Wizard

After you click on the *Finish* button, a window will display asking if you want to add the certificate to the Root Store. The certificate is detailed in this window, as shown in figure 15 below.

Click on **Yes** when the Root Certificate Store window displays.

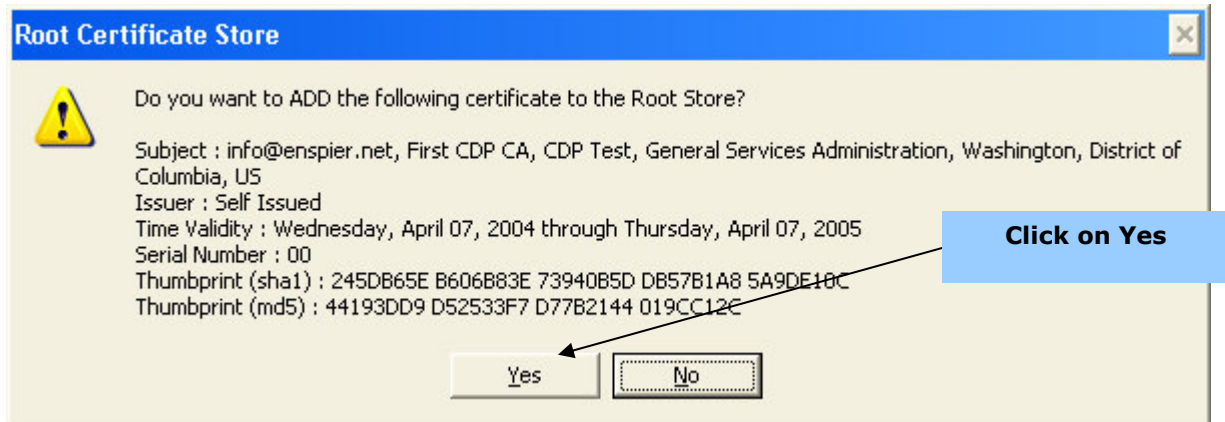


Figure 10-15: Root Certificate Store

If the import wizard worked, and the certificate was imported into your browser, a notification window will display, as shown in figure 10-16.



Figure 10-16: Complete the Import Wizard

3 Configure IIS server for SSL with Client Authentication

Before attempting to obtain a Certificate Authority server certificate, use section 3.1 to create a certificate request. Once the request is created, send it to your Agency Relationship Manager and proceed to section 3.2.

3.1 Create a Server Certificate Request

The first step for creating a server certificate request is running Internet Services Manager. Goto:

- Start
- Programs
- Administrative Tools
- Internet Services Manager

After you click on Internet Services Manager, an *Internet Information Services* screen will display, as shown below.

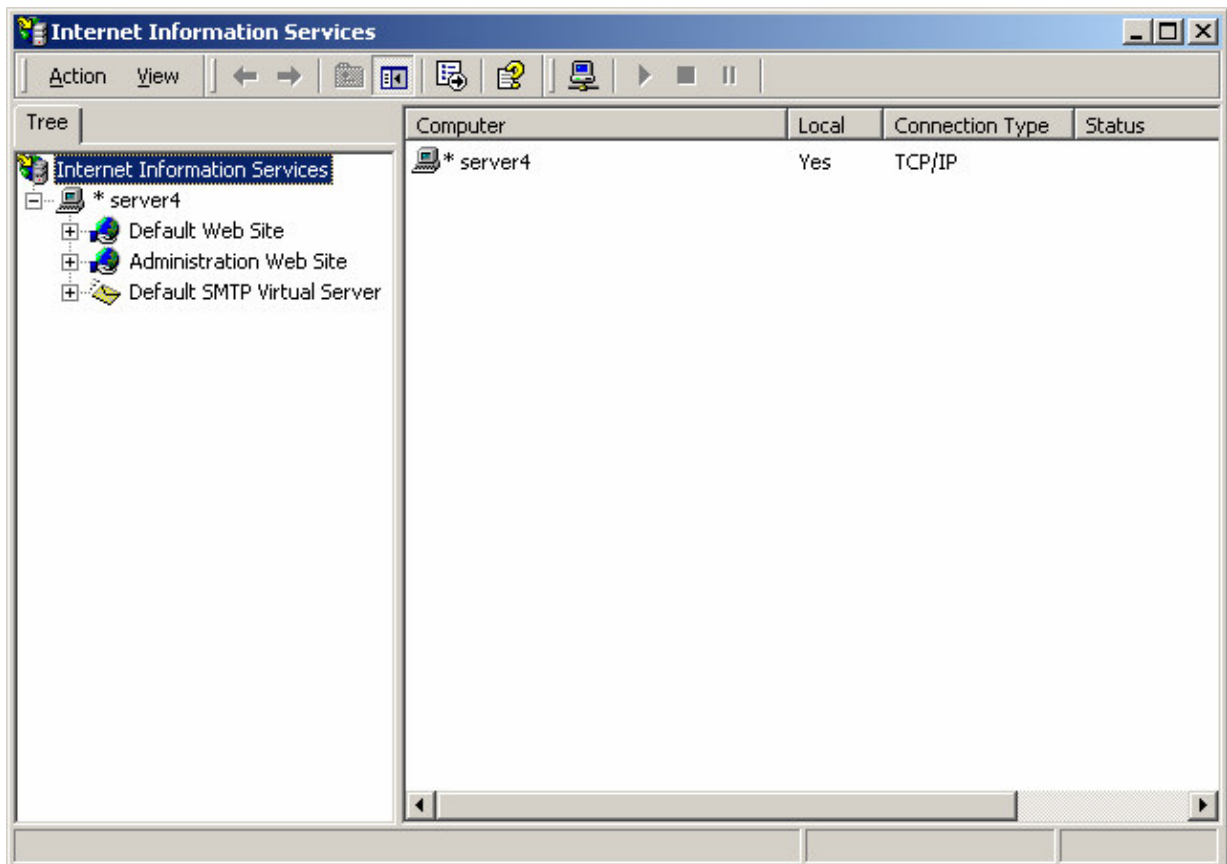


Figure 10-17: Complete the Import Wizard

Choose the Server name and the web site you want to configure by navigating the left pane. Right click on the server you will configure. Ensure that the IIS sever is not running, and click on *Stop* if so.

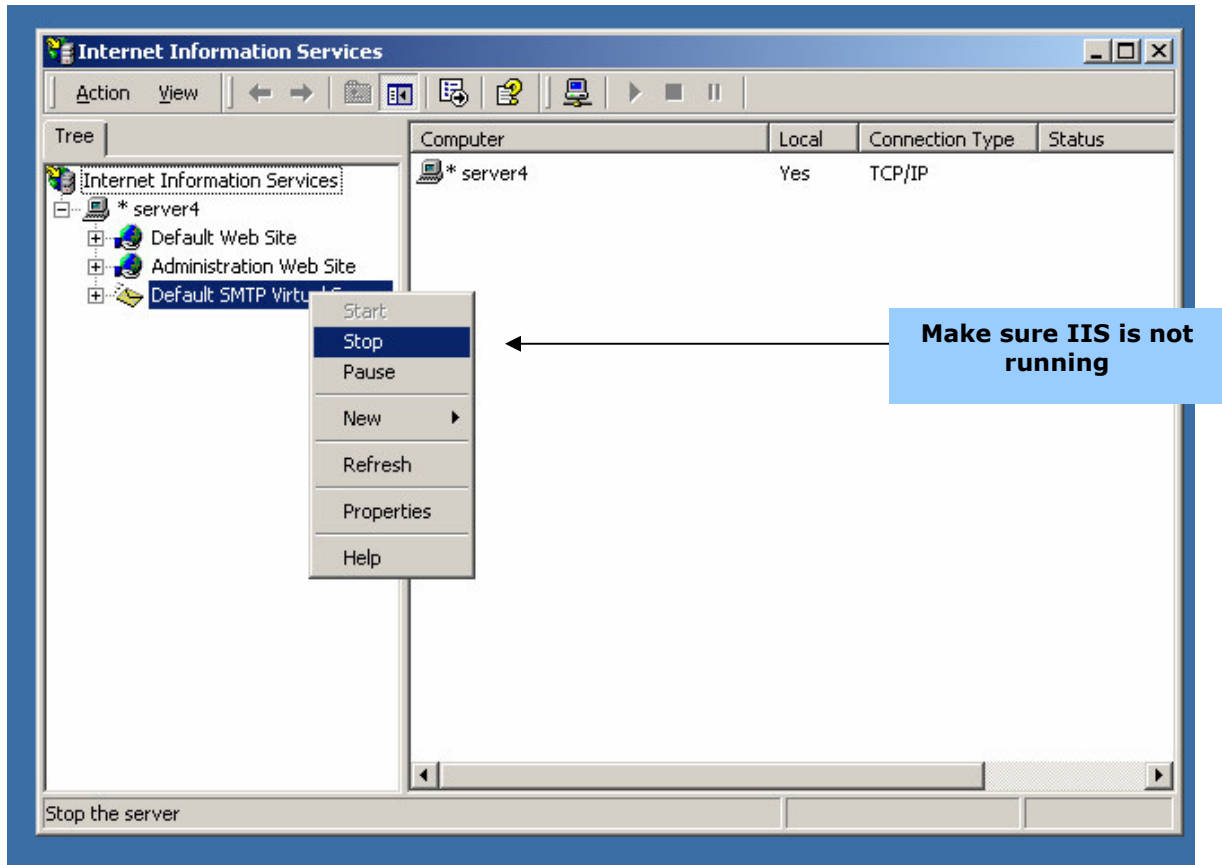


Figure 10-18: Complete the Import Wizard

Right click on the website you want to configure and click on *Properties*. A window with website properties will display, as shown in Figure10-19. Once the web site properties window displays, click on the *Directory Security* tab and click on the *Edit* button.

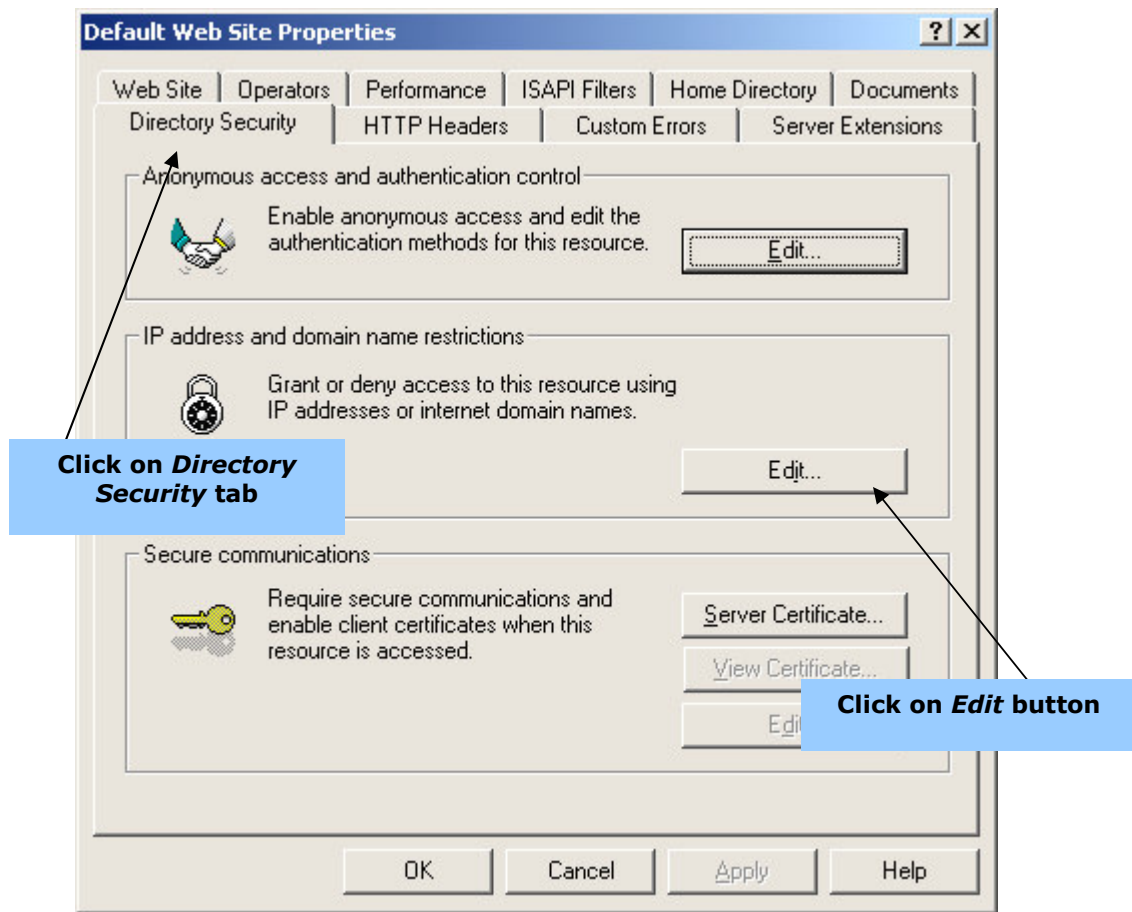


Figure 10-19: Complete the Import Wizard

After you click on the *Edit* button, the window shown below will display.

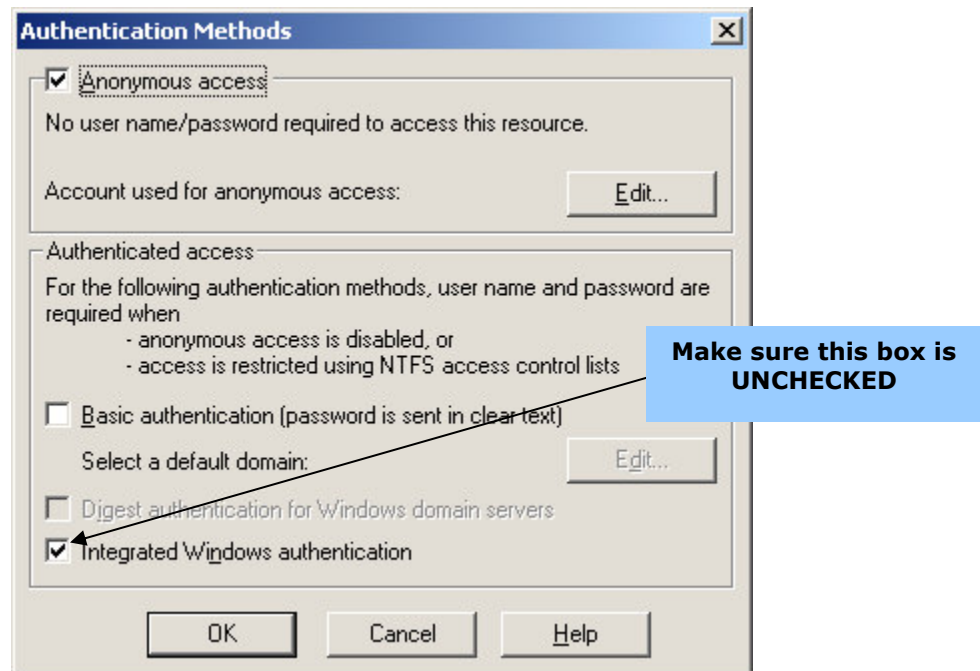


Figure 10-20: Authentication Methods

Clear the *Integrated Windows Authentication* checkbox, and then click *OK*. You will be back at the web site properties dialogue box, displayed in figure 10-19, above. Next, click on *Server Certificate*.

Web Server Wizard will appear, as shown in figure 10-21 below. The Web Server Certificate Wizard will automate some of the steps for creating server certificate requests. When figure 21 displays click *Next*.

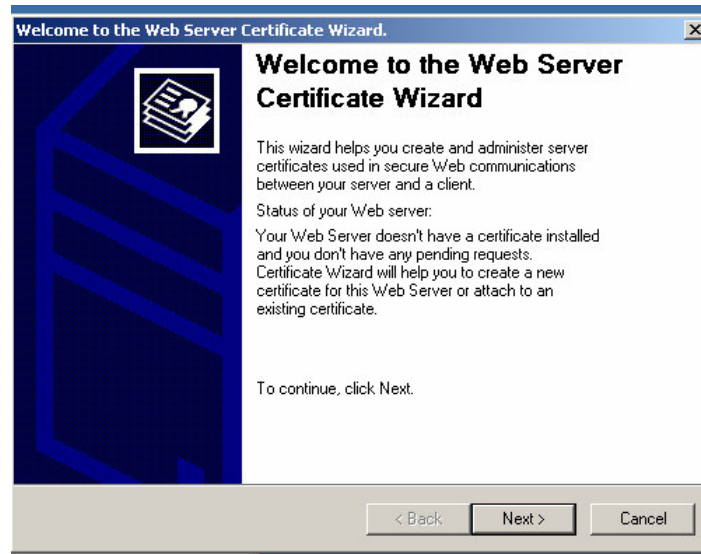


Figure 10-21: Web Server Certificate Wizard

There are three methods for assigning a certificate to a Web site. Make sure you select *Create a new certificate* and then hit the *Next* button.

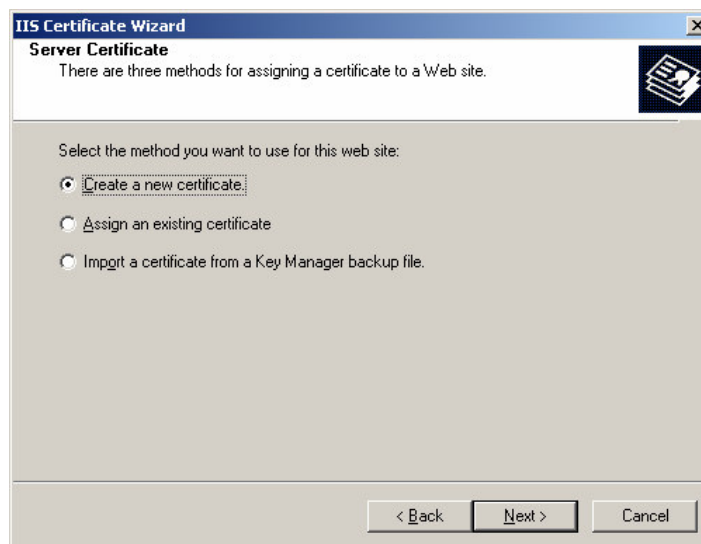


Figure 10-22: Web Server Certificate Wizard

Select *Prepare the request now, but send it later* and then click on the *Next* button. The Name and Security Settings window will display.

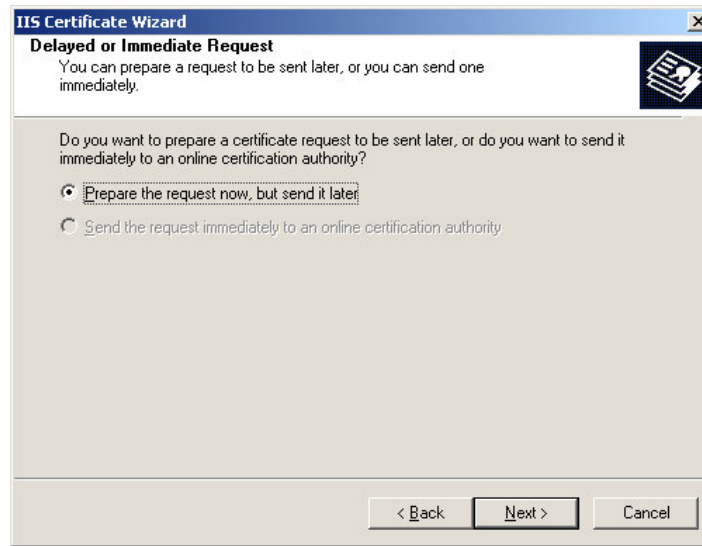


Figure 10-23: Delayed or Immediate Request

Choose an easy to remember name for the website for which you want to create the certificate. Select a bit length of 2048, then click on the *Next* button.

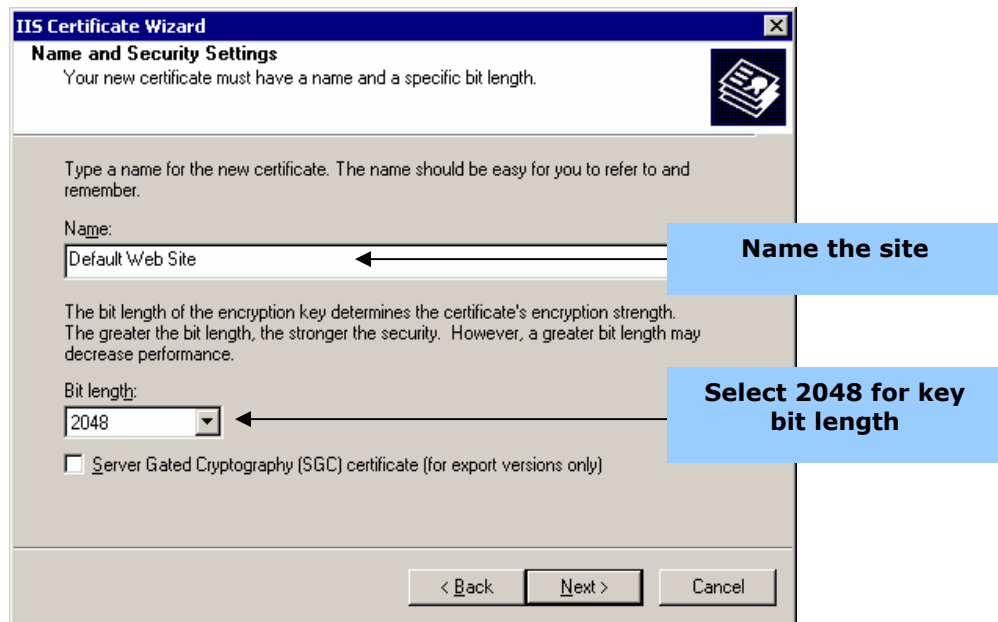
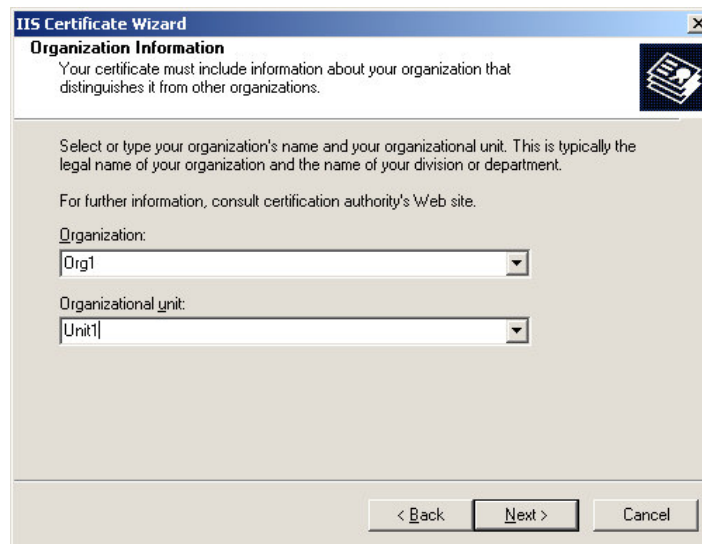


Figure 10-24: Name and Security Settings

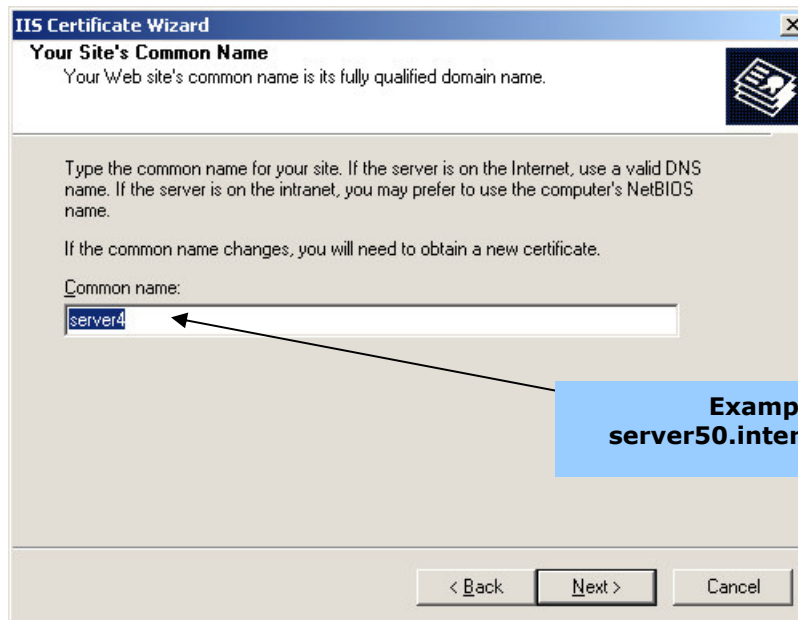
Your certificate must include information about your organization that makes it easier to distinguish it from similar organizations. Select or type your organization's name and your organizational unit or department, then click *Next*.



The screenshot shows the 'IIS Certificate Wizard' window with the 'Organization Information' tab selected. The window title is 'IIS Certificate Wizard'. The main heading is 'Organization Information'. Below the heading, there is a sub-heading 'Your certificate must include information about your organization that distinguishes it from other organizations.' followed by a small icon of a document with a magnifying glass. The text instructs the user to 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' and 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with 'Org1' selected, and 'Organizational unit:' with 'Unit1' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 10-25: Organization Information

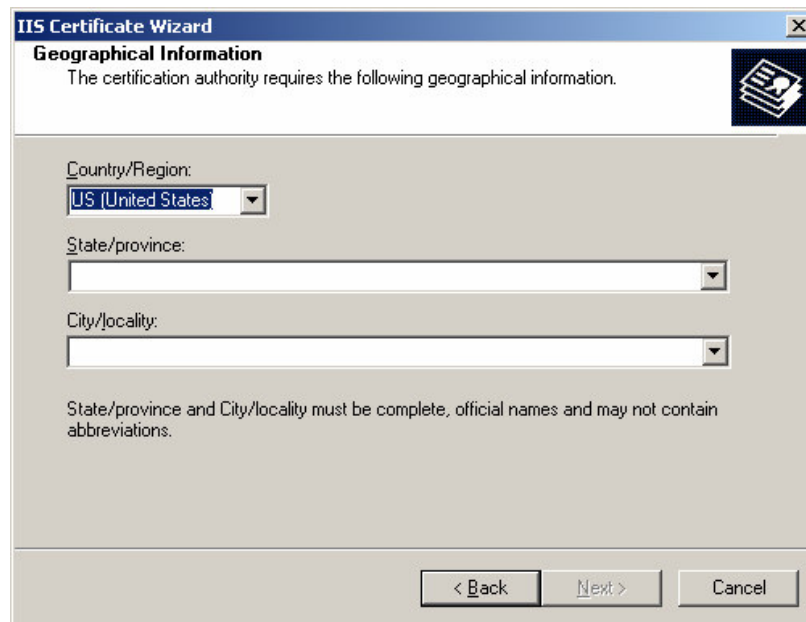
Select a common name, but ensure that this is the full DNS name of the server. Click on *Next* after you choose a name. **Example: server50.interoplab.gov**



The screenshot shows the 'IIS Certificate Wizard' window with the 'Your Site's Common Name' tab selected. The window title is 'IIS Certificate Wizard'. The main heading is 'Your Site's Common Name'. Below the heading, there is a sub-heading 'Your Web site's common name is its fully qualified domain name.' followed by a small icon of a document with a magnifying glass. The text instructs the user to 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' and 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' with the text 'server4' entered. A blue callout box with an arrow pointing to the input field contains the text 'Example: server50.interoplab.gov'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 10-26: Your Site's Common Name

Fill out information about your location, and then click on *Next*.



The screenshot shows a Windows-style dialog box titled "IIS Certificate Wizard". The main heading is "Geographical Information". Below the heading, a message states: "The certification authority requires the following geographical information." To the right of this text is a small icon of a document with a keyhole. The form contains three dropdown menus: "Country/Region:" with "US (United States)" selected, "State/province:", and "City/locality:". Below these fields, a note reads: "State/province and City/locality must be complete, official names and may not contain abbreviations." At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Figure 10-27: Geographic Information

After you enter your geographic information, you will be prompted to enter a filename for the certificate request. Choose a name or browse to find the most desirable location to store this file.

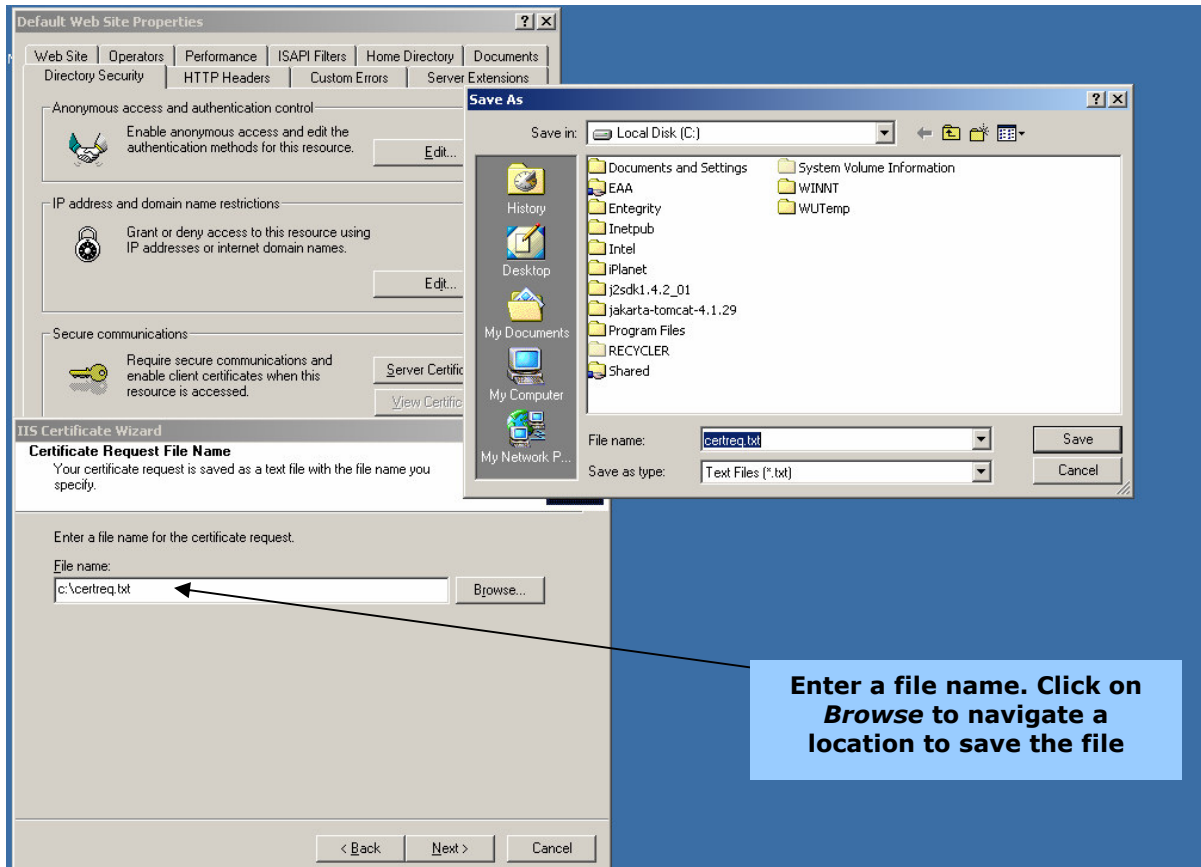


Figure 10-28: Certificate Request File Name

After you name the file and location, you will have an opportunity to review the information you entered. To change something, click on the *Back* button, otherwise click on *Next*.

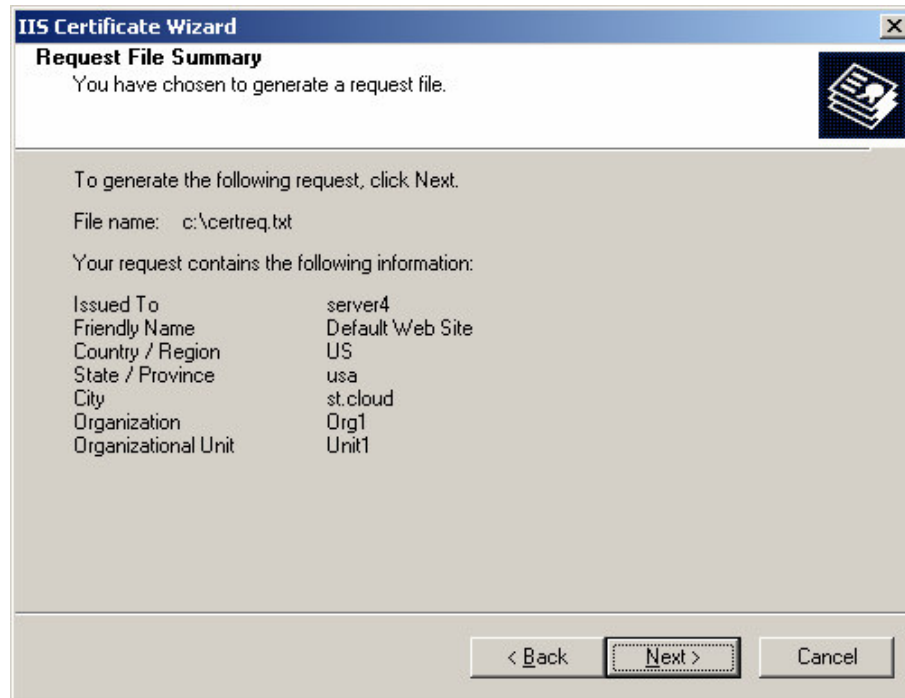


Figure 10-29: Request File Summary

When you are satisfied with the information you entered, click on *Finish* to exit the certificate wizard.



Figure 10-30: Finish the Cert Wizard

3.2 Import Server Certificate into IIS

Before you can begin section 3.2, send the certificate request created in 3.1 to your CA. Save the certificate returned by the CA in an appropriately named file, for example, **c:\cert1.cer**

After you have the certificate returned by the CA, you will import a server certificate into IIS by running Internet Services Manager. Select:

- Start
- Programs
- Administrative Tools
- Internet Services Manager

After you click on Internet Services Manager, an *Internet Information Services* screen will display, as shown below.

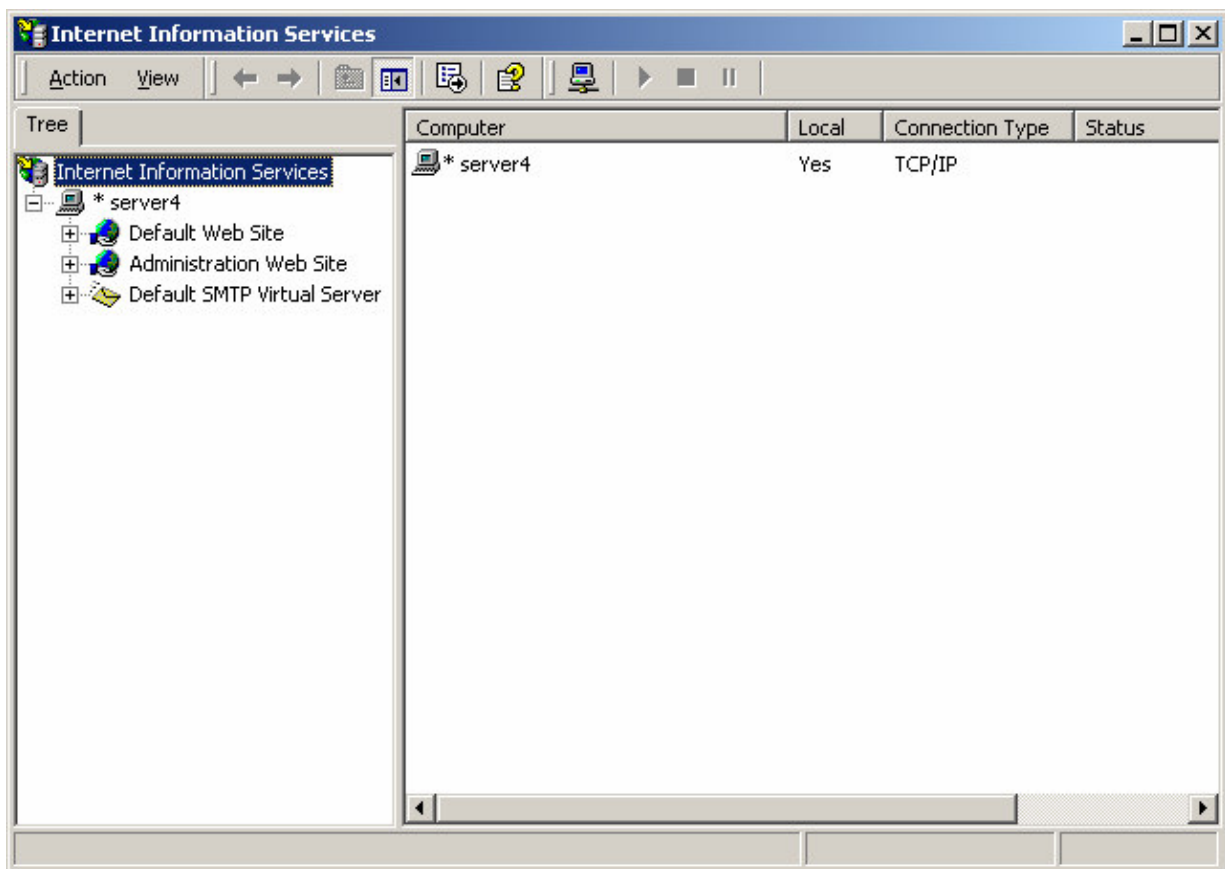


Figure 10-31: Complete the Import Wizard

Choose the Server name and the web site you want to configure by navigating the left pane. Right click on the server you will configure. Ensure that the IIS sever is not running, and click on *Stop* if so.

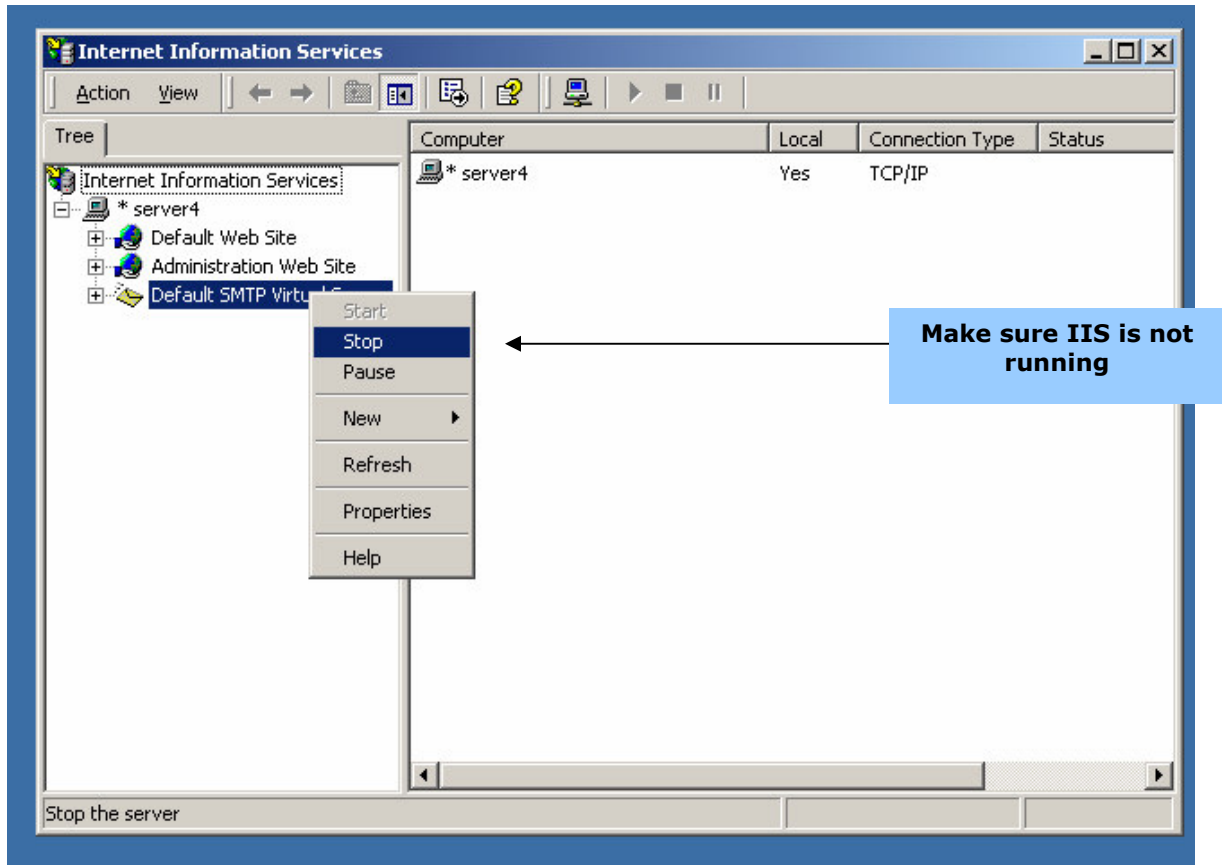


Figure 10-32: Complete the Import Wizard

Right click on the website you want to configure and click on *Properties*. A window with website properties will display, as shown below. Once the web site properties window displays, click on the *Directory Security* tab.

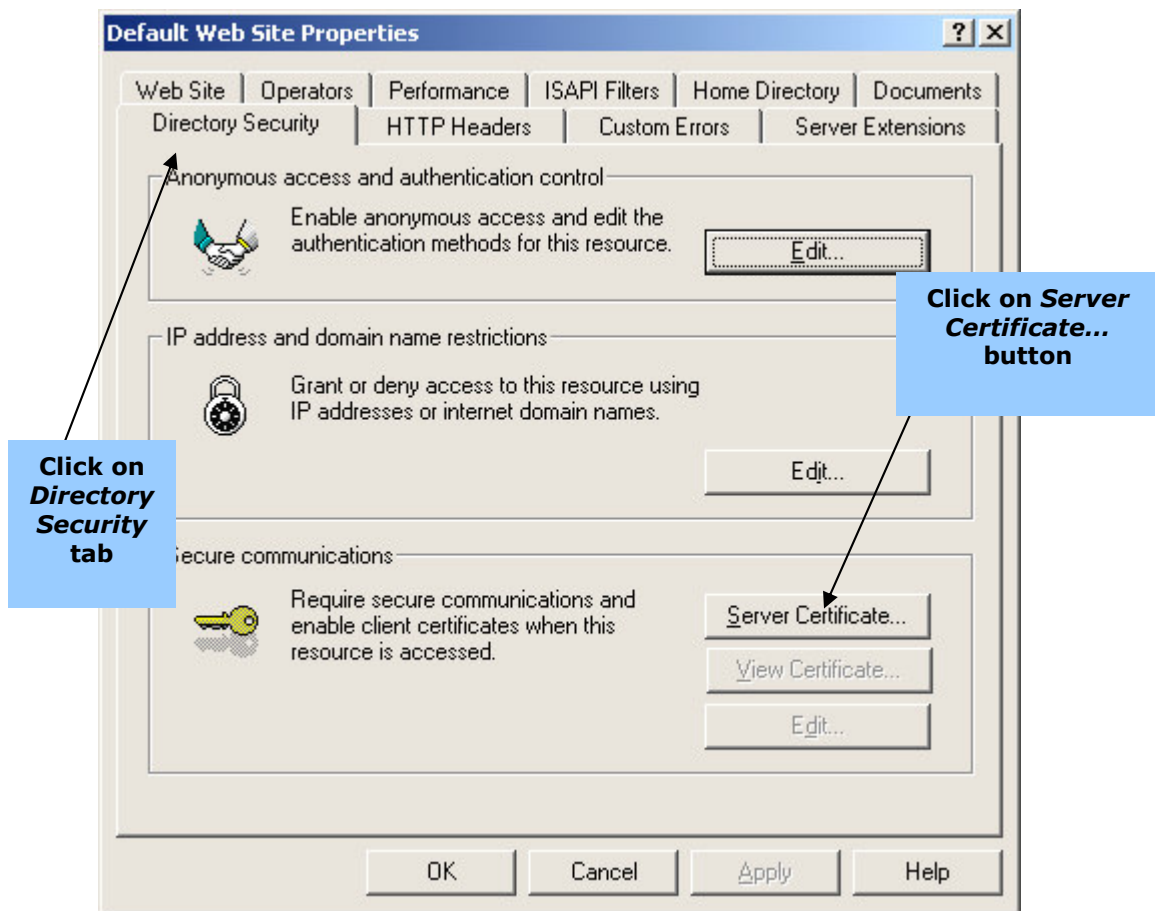


Figure 10-33: Complete the Import Wizard

Once in the *Directory Security* section, click on the *Server Certificate* button. The Web Server wizard will appear, click *Next* and follow the steps below.

- Select *Process the pending request and install the certificate*, then click *Next*.
- Enter path name of the file containing the certification authority's response, click *Open*.
- Click *Next*.
- Click *Finish*.
- Click *Edit* in the *Secure Communications* section.
- Click *Require secure channel SSL*, click *require 128-bit encryption*.
- Click *Require client certificates*, and then click *OK*.
- After you click *OK*, click on *Web site* tab. The SSL port has been changed to 443.
- For inheritance overrides, click *OK*
- Click *OK*
- Stop and then start IIS